14 Probabilistische Methoden II

Def: (Ω, P) Wahrscheinlichkeitsraum:

- Ω endliche Menge
- $P: \Omega \to \mathbb{R}$ mit
  - $P(\omega) \geq 0$ für $\omega \in \Omega$
  - $\sum_{\Omega} P(\omega) = 1$
- $A \subseteq \Omega$ heißt Ereignis, $P(A) := \sum_{\omega \in A} P(\omega)$

$\rightsquigarrow P: 2^{\Omega} \to \mathbb{R}$, $P(\Omega) = 1$

→ oft: abgeleitete Informationen:

Def: <u>Zufallsvariable</u> $X: \Omega \to \mathbb{R}$

$$P(X = x) = \sum_{\omega \in \Omega,\, X(\omega) = x} P(\omega)$$

$\rightsquigarrow$ $X = x$ ist Ereignis im abgeleiteten Wahrscheinlichkeitsraum $\{X(\omega) \mid \omega \in \Omega\}$

<u>Bsp</u>: Anzahl „Kopf" bei n-fachem Münzwurf.

<u>Def</u> <u>Erwartungswert</u> von X

$$\mathbb{E}[X] := \sum_{\omega \in \Omega} X(\omega) P(\omega) = \sum_{x \in \mathbb{R}} x P(X = x)$$

Summe ist endlich, da $X(\omega)$ endlich

Def: Zufallsvariablen X, Y sind <u>unabhängig</u>

$\iff \forall x, y \in \mathbb{R}: P(X = x \text{ und } Y = y) = P(X = x) P(Y = y)$

Prop: $\mathbb{E}$ ist linear:

$$\mathbb{E}[\alpha X] = \alpha\,\mathbb{E}[X], \quad \mathbb{E}(\textstyle\sum X_i) = \sum \mathbb{E}(X_i)$$ ☒

Prop: X, Y unabhängig, dann $\mathbb{E}[XY] = \mathbb{E}[X]\,\mathbb{E}[Y]$ ☒

Satz (Markovungleichung)

$X \geq 0$, $t \geq 0$. Dann

$$P(X \geq t) \leq \frac{1}{t}\,\mathbb{E}[X]$$

$\ulcorner$ $$\mathbb{E}[X] = \sum_{a \geq 0} a\,P(X=a)$$

$$\geq \sum_{a \geq t} a\,P(X=a) \geq \sum_{a \geq t} t\,P(X=a) = t\,P(X \geq t)$$ $\lrcorner$

Satz $G=(V,E)$ Graph mit $2n$ Knoten, $m > 0$ Kanten

Dann gibt es Partition $V = A \,\dot\cup\, B$ mit $|A| = |B| = n$, so dass $\geq m/2$ Kanten zwischen A und B verlaufen.

$\ulcorner$ Wählen A zufällig $\rightsquigarrow \binom{2n}{n}$ Möglichkeiten

$\rightsquigarrow$ alle gleich wahrscheinlich

$B := V \setminus A$

$X : \{A\} \to \mathbb{Z}$ Anzahl Kanten innerhalb von A, B

Für $e \in E$: C_e Ereignis, dass $|A \cap e| = |B \cap e| = 1$

Dann: $X = \sum (1 - I_{C_e})$ Indikatorvariablen

$$\Rightarrow \quad \mathbb{E}[X] = m - \sum_{E} P(C_e)$$

$\rightsquigarrow$ bestimmen $P(C_e)$

$e = uv$: $u \in A, v \notin A$, Rest kann auf $\binom{2n-2}{n-1}$ Arten verteilt werden

$u \notin A, v \in A$ analog

$$\Rightarrow P(C_e) = \frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1} > \frac{1}{2}$$

$$\Rightarrow \mathbb{E}[X] < m - \frac{m}{2} = \frac{m}{2} \Rightarrow P\left(X \geq \frac{m}{2}\right) < \frac{2}{m}\frac{m}{2} = 1$$

$\lrcorner$

Def $M \subseteq \mathbb{Z}$ heißt summenfrei, wenn $x+y \notin M$ für alle $x, y \in M$.

$\to$ $S \subseteq \mathbb{Z}$, wie groß kann eine summenfreie Menge $M \subseteq S$ sein?

Bsp $S = [2n]$, dann: $M_1 = \{n+1, \dots, 2n\}$
$M_2 := \{a \in S \text{ ungerade}\}$

summenfrei $\to |M| = \frac{1}{2}|S|$

Satz $S \subseteq \mathbb{Z} \setminus \{0\}$. Dann gibt es $M \subseteq S$ summenfrei mit $|M| \geq \frac{1}{3}|S|$

$\ulcorner$ Wähle p prim, $p > |a|$ für alle $a \in S$

Setze $A := \{ \lceil \frac{p}{3} \rceil, \dots, \lfloor \frac{2}{3}p \rfloor \} \subseteq \mathbb{Z}_p$

$\Rightarrow$ $|A| \geq \frac{1}{3}(p-1)$

A ist summenfrei in $\mathbb{Z}_p$

$\rightarrow$ wähle $x \in \mathbb{Z}_p \setminus \{0\}$ zufällig

$\rightarrow$ setze $S_x := \{ a \in S \mid ax \ (\mathrm{mod}\ p) \in A \}$

$\rightarrow$ $a, b \in S_x$, dann:

$$ax + bx \equiv (a+b)x \ (\mathrm{mod}\ p)$$

$\Rightarrow$ $a+b \notin S_x$, da A summenfrei

$\Rightarrow$ S_x ist summenfrei

$\rightarrow$ setze: $X : \mathbb{Z}_p \setminus \{0\} \rightarrow \mathbb{Z}, \quad x \mapsto |S_x|$

und $\chi_x(m) := \begin{cases} 1 & m \in S_x \\ 0 & \text{sonst} \end{cases}$

Dann:

$$X = \sum_{m \in S} \chi_x(m)$$

$$P(mx \ (\mathrm{mod}\ p) \in A) = \frac{|A|}{p-1} \geq \frac{1}{3}$$

$$\Rightarrow \mathbb{E}[X] = \mathbb{E}\Big[\sum_{m \in S} \chi_x(m)\Big] = \sum_{m \in S} \mathbb{E}[\chi_x(m)]$$

$$= \sum_{m \in S} P(mx \ (\mathrm{mod}\ p) \in A) \geq \frac{1}{3}|S|$$

$\Rightarrow$ es gibt x mit $|S_x| \geq \frac{1}{3}|S|$ $\square$

→ Idee der prob. Methode

(1) es gibt wenige „schlechte" Ereignisse $A_1, \dots, A_k$

wenn $P(\bigcup A_i) \leq \sum P(A_i) < 1$

→ es muss „gutes" Ereignis geben.

(2) schärfer:

A, B unabhängig, „schlechte" Ereignisse

$\to P(\bar{A} \cap \bar{B}) = P(\bar{A}) P(\bar{B})$

Das ist > 0, wenn $P(\bar{A}), P(\bar{B}) > 0$

⇒ es gibt „gutes" Ereignis

<u>aber</u>: nur richtig, wenn A, B unabhängig!

<u>Def</u> B ist <u>stochastisch unabhängig</u> von $A_1, \dots, A_k$, wenn für jedes $I \subseteq [k]$ B unabhängig von $\bigcap_{i \in I} A_i$ ist

<u>Bsp</u> Folge von Münzwürfen

A_1: erster Wurf ist Zahl

A_2: letzter — " —

B: erster und letzter Wurf sind gleich

$\to P(B \mid A_1) = P(B \mid A_2) = P(B) = \frac{1}{2}$

aber $P(B \mid A_1 \cap A_2) = 1 \neq P(B)$

⇒ B ist <u>nicht</u> stochastisch unabhängig

$\Rightarrow$ können wir (1) verbessern, wenn die $A_1, \dots, A_k$ „fast" stochastisch unabhängig sind?

Satz (Lovasz local lemma)

$A_1, \dots, A_k$ Ereignisse, $P(A_i) \leq p$ für alle i

Es gibt d: A_i stoch. unabh. von $\{A_j \mid j \in J\}$ für ein $J \subseteq [k] \setminus \{i\}$, $|J| \geq k-d-1$

Wenn $4pd < 1$, dann $P(\bigcap \overline{A_i}) > 0$

⌈ohne Beweis⌋

Satz $\mathcal{F}$ r-uniforme Mengenfamilie in $2^{[n]}$

Jedes $A \in \mathcal{F}$ hat nichtleeren Schnitt mit $m < 2^{r-3}$ anderen Mengen in $\mathcal{F}$

$\Rightarrow \mathcal{F}$ ist 2-färbbar.

⌈ $\mathcal{F} = \{M_1, \dots, M_k\}$ färbe Grundmenge zufällig rot/blau

A_i: Ereignis, dass M_i nur eine Farbe hat

$\Rightarrow P(A_i) = \frac{1}{2^{r-1}} =: p$

A_i ist unabh. von A_j, wenn $M_i \cap M_j = \emptyset$

$d := m < 2^{r-3} \Rightarrow A_i$ stoch. unabh. von allen außer d der A_j

$4pd < 4 \cdot \frac{1}{2^{r-1}} 2^{r-3} = 1 \overset{\text{LLL}}{\Rightarrow} P(\bigcap \overline{A_j}) > 0$

$\Rightarrow$ es gibt Färbung ⌋

Beweis des Lovasz local Lemma:

Beh: für jedes m und jede Auswahl von m der A_i (nach Umnummerieren $A_1, \dots, A_m$) gilt

$$P(A_1 \mid \bar{A}_2 \cap \dots \cap \bar{A}_m) \leq 2p$$

Induktion über m: $m = 1$ ✓

$m \geq 2$: können annehmen, dass A_1 stoch. unabh. von $A_{k+1}, \dots, A_m$ für ein $k \leq d+1$

Aus $P(A \mid B \cap C) = \frac{P(A \cap B \mid C)}{P(B \mid C)}$ folgt

$$P(A_1 \mid \bar{A}_2 \cap \dots \cap \bar{A}_m) = \frac{P(A_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_k \mid \bar{A}_{k+1} \cap \dots \cap \bar{A}_m)}{P(\bar{A}_2 \cap \dots \cap \bar{A}_k \mid \bar{A}_{k+1} \cap \dots \cap \bar{A}_m)} \quad (*)$$

Nun gilt

$$P(A_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_k \mid \bar{A}_{k+1} \cap \dots \cap \bar{A}_m) \leq P(A_1 \mid \bar{A}_{k+1} \cap \dots \cap \bar{A}_m)$$
$$\leq P(A_1) \leq p$$

$$P(\bar{A}_2 \cap \dots \cap \bar{A}_k \mid \bar{A}_{k+1} \cap \dots \cap \bar{A}_m) = 1 - P(A_2 \cup \dots \cup A_k \mid \bar{A}_{k+1} \cap \dots \cap \bar{A}_m)$$
$$\geq 1 - \sum_j P(A_j \mid \bar{A}_{k+1} \cap \dots \cap \bar{A}_m)$$
$$\geq 1 - (k-1) 2p \geq 1 - 2pd \geq 1/2$$

$$\Rightarrow \text{in } (*) \; P(A_1 \mid \bar{A}_2 \cap \dots \cap \bar{A}_m) \leq \frac{p}{1/2} = 2p$$

Nun gilt $P(A \cap B \cap C) = P(A \mid B \cap C) P(B \mid C) P(C)$

$$\Rightarrow P(\cap \bar{A}_i) = \prod_{i=1}^{k} P(\bar{A}_i \mid \bar{A}_1 \cap \dots \cap \bar{A}_{i-1}) \geq (1-2p)^k > 0$$